| | |
|---|---|
| **Section V:** | **Physical Security** |
| **Title:** | **Site Security Plan Standard** |
| **Current Effective Date:** | **June 30, 2008** |
| **Revision History:** | **May 16, 2008** |
| **Original Effective Date:** | **June 30, 2008** |

**Purpose:** To provide guidance on key areas that shall be addressed by a facility when developing a comprehensive and effective facility security plan.

# STANDARD

## 1.0 Background

Physical security provides for the protection of property, personnel, and facilities against unauthorized entry, trespass, damage, sabotage, or other criminal acts. The Site Security Plan deals with prevention and control of access to the building, data, and the information technology (IT) resources contained therein.

## 2.0 Physical Facility Controls

### 2.1 Perimeter Security Controls

A risk assessment shall be performed to determine the level of security needed to mitigate vulnerabilities to the exterior of a facility. Risk assessments shall be conducted in accordance with North Carolina (NC) Department of Health and Human Services (DHHS) Security Standards, Administrative Security - Information Security Risk Management Standard. Based on the level of risk involved, parking barriers or restrictions may need to be imposed to limit the access of vehicular traffic to the immediate exterior of a facility. It may also be necessary to implement some proximity controls such as exterior lighting or video monitoring in order to increase visibility of entryways.

## 3.0 Facility Access and Security Controls

All facilities shall have some form of an after-hours intrusion detection system. The type and complexity of the system required will be identified by a risk assessment as identified in section 2.0 of this standard. The access controls chosen may be as simple as periodic security patrols or a local system consisting of entry contact sensors with audible alarms. The system can also be as comprehensive as magnetic contact points with penetration, motion, and/or heat detection sensors linked into a centrally monitored security network. Items such as facility design, business function, and risk should all be considered when determining the level of protection necessary for each Division or Office.

To provide access monitoring of workforce members and visitors alike, certain controls shall be used. One method of access control is to have a manned reception desk at a single entrance location. This allows for positive identification of both workforce members and visitors and provides the opportunity to use a visitor sign-in log, escorts, and unique visitor badging. Other methods of facility access control such as magnetic or radio frequency (RF) identification cards and personal identification numbers (PIN) may be implemented to control and restrict entry into a facility and allow for access audits. The main objective of the facility access control method chosen is to eliminate all points of uncontrolled entry.

### 3.1 Defining Secure Areas

A secure area is any location identified by the Division or Office where security controls shall be applied to reduce unauthorized access or any other type of security risks. All secure areas must be documented and monitored routinely in accordance with the security standards defined in the NC DHHS Security Standards, Administrative Security - Information Security Risk Management Standard. Signs indicating that specific authorization is required for access to a secure area shall be conspicuously posted at any and all entry points.

### 3.2 Access to Secure Areas

All workforce members that are granted access to a secure area shall be documented on an authorized access roster maintained by a Division or Office workforce member. Secure areas used for IT/network equipment, data processing, or storage of protected information shall always be located in an easily monitored location. When temporary access to secure areas is required for non-workforce personnel, a sign in/out log and escort process shall be implemented.

### 3.3 Issuance of Access Devices/Codes

When it is necessary to issue keys, combinations, or access codes, an assignment register or list shall be used. Some method of signature receipt shall also be implemented. This provides documentation that an individual has received such items and informs the user of their responsibilities. Upon change in employment status or termination, employees will be required to return any issued items and signify that they have been returned. When an individual no longer requires a combination or access code, the code shall be changed within one working day of the individual's termination or change of status.

## 4.0 Administration and Support Systems

Monitoring of workforce members and visitors is an important component of information protection. Any monitoring by video surveillance or RF badging shall be implemented in a way that does not intrude on an individual's personal privacy. Monitoring shall only provide a means of verifying activity in common areas, entry/exit locations, and accessing information systems or areas that contain information systems. Exceptions to this rule would include those cases where it is deemed necessary to monitor individuals as a part of the organizations normal operations. Full disclosure of such monitoring shall be part of an initial security training program. Areas where unauthorized access is prohibited or video monitoring is used shall be clearly identified.

### 4.1 Training and Awareness

An individually tailored security training and awareness program shall be implemented. Initial training shall encompass all aspects of the security program a Division or Office uses. Subsequent periodic training shall be used on an as needed basis. New procedures, changes to policy, or new threat awareness training shall be communicated to all workforce members when circumstances require. All training, either initial or periodic, shall be documented and copies retained in either personnel folders or designated security folders to substantiate proof of awareness.

### 4.2 End of Day Process

End of day security checks are a vital part of protection against inadvertent disclosure of information. An end of day check involves visually inspecting all printers, faxes, and copiers for sensitive information that may have been left by a user. Except for systems requiring uninterrupted network connectivity, or in cases of pending maintenance or patching, all systems shall be turned off or be put into a hibernation state while the facility is unoccupied. If appropriate and warranted by a risk assessment, an end of day check may be documented by the last individual to leave an area or facility and retained for a period of no less than ninety (90) days. If used, a documented end of day check shall be tailored to the specific requirements of the facility, division, or office and shall be as simple as possible while providing an adequate level of verifiable monitoring.

### 4.3 Facility Architectural Plans

Facility, infrastructure, environmental, network, and IT system designs/plans shall be secured and maintained by designated facility or security personnel so they are readily available for future planning, organization, or facility restructuring. These plans are also a critical cross reference tool for configuration management and for use by outside personnel in the event of an emergency, disaster, or other major disruption to normal operations.

## 5.0 Power, Data and Environmental Controls

### 5.1 Power, IT, Networks, and Data Systems

Space, power, and HVAC requirements shall be carefully planned to meet the needs of the operation and afford the necessary level of protection. When planning for new or rehabilitative construction, proper planning, documentation, and design shall be coordinated with security, maintenance, and IT systems personnel. IT, network, communications, data storage and backup requirements must be planned and located appropriately to afford the required level of protection. IT, network, and storage security will be based on the level of risk identified by an organization. Equipment necessary for continuity of operations shall be located in secure areas with either electronically or manually controlled access. Other equipment useful for daily operations but not required for continuity of business shall be located in an area that inhibits public access and is visually monitored during operating hours. Communications hubs such as telephone trunks and Voice over Internet Protocol (VoIP) equipment shall be located in an area that restricts unauthorized access. Network wiring shall be located in secure network closets, routed above ceilings or beneath flooring, inaccessible to the public, and enclosed in solid conduit to reduce the threat of tampering.

### 5.2 Facility and System Environmental Control Documentation

Some Divisions and Offices may need network data centers or climate controlled server rooms to conduct their operations. Requirements for lighting, water supply, fire suppression, and HVAC systems shall be coordinated with security personnel to develop systems that pose as little vulnerability to sensitive data as possible. Most exposure, accessibility, or tampering threats can be mitigated with proper planning, location, and access controls.

### 5.3 Off Site/On Site Power Generation, Location, Accessibility, and Alternatives

Proper security of electronic data and equipment relies on an available and consistent source of power. Based on an organization's operational and power consumption needs and its location within a primary or secondary source of electrical power, an on-site backup generation capability may need to be implemented. Organizations with critical operations will require the use of automatic crossover to backup power generators. Organizations with noncritical but sustained operational requirements may only need the availability of manual generator capability to power essential equipment. All IT infrastructure, data processing, and storage systems shall be powered through an uninterruptable power supply (UPS) surge protection device. This provides time to secure and shut down electronic equipment in the event of an outage without damage or loss of data until a secondary source of power can be established. Primary and secondary paths of service shall be documented, maintained, and tested periodically to ensure availability.

## 6.0 Security Documentation and Maintenance Records

Facility risk assessment and historical incident documentation shall be maintained and reviewed to define the foundation needed to develop and implement appropriate protections. Review of incident documentation will help to formulate new processes or procedures to minimize the risk of recurrence.

### 6.1 Facility and System Maintenance Requirements/Contract Documentation

Any required system testing or information backup processes for IT infrastructure systems shall be documented and available for inspection and use during situations such as suspected unauthorized access or data loss. Items documented shall, at a minimum, include the following:

- Times
- Dates
- Frequency

Any local or state agency contract documents for maintenance and upgrade of facilities shall be retained for future safety, security, and legal reference.

### 6.2 Maintenance and Test Schedules

All Divisions and Offices shall identify and define periodic maintenance schedules and test requirements for systems such as fire and intrusion alarms, emergency equipment, or notification procedures. While facility function will dictate the policies implemented, both announced and unannounced alarm testing shall be done to determine realistic results. All maintenance and test procedures, as well as results, must be documented and maintained for safety, security, and legal reference as well as identifying areas for improvement and steps taken to eliminate risks.

Self-assessments shall be conducted to provide a warning flag to management so problems can be addressed before they arise in maintenance or test reports. Self-assessments may be performed by operations personnel or by vendors under the direction of those at the facility who are responsible for the systems being assessed. Self-assessments may use tools and techniques such as checklists, audits, penetration tests, visual observation, etc. Additional resources used to conduct a self-assessment may include, but are not limited to, the following:

- Reviewing previous test, audit, and self-assessment results
- Assessing conformance to policies, procedures, and prior corrective actions
- Scanning facility entrances and access points for vulnerabilities
- Verifying that devices and networks are located in protected areas
- Ensuring inventories and asset status changes are properly documented and reviewed
- Verifying that hard and soft data are stored only where authorized
- Reviewing the adequacy of the risk assessment and monitoring plans

## Reference:

- NC Statewide Information Technology Security Manual, Version No. 01 - Chapter 3 - Processing Information and Documents
  - Section 02: System Operation and Administration
    - Standard 030215 - Commissioning Facilities Management for Information Technology
- NC Statewide Information Technology Security Manual, Version No. 01 - Chapter 5 - Securing Software, Peripherals and Other Equipment
  - Section 02: Cabling, UPS, Printers and Modems
    - Standard 050202 - Managing and Maintaining Backup Power Generators

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Physical and Environmental Security Policy
  - Security Testing Policy

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Risk Management Standard